Informationen zu Datenschutz und Sicherheit mit CYS Feedback Monitor (CFM)

Technische Sicherheitsvorkehrungen

Hosting über Microsoft Azure

CFM-Systeme und Daten werden in den professionellen Rechenzentren von Microsoft Azure gehostet. Microsoft Azure hat mehr Zertifizierungen (u.a. ISO) als jeder andere Cloudanbieter. 90 Prozent aller Fortune 500-Unternehmen vertrauen der Microsoft Cloud. Detaillierte Informationen können bei Bedarf zur Verfügung gestellt werden. (Wie z.B. aktuelle Zertifikate, Sicherheitspläne etc.)

- **Allgemeine Informationen zu Microsoft Azure:**

  https://azure.microsoft.com/de-de/overview/what-is-azure/

- **Azure Deutschland (Cloud Computing, Sicherheit, T-Systems als Datentreuhänder):**

  https://azure.microsoft.com/de-de/overview/clouds/germany

- **Weitere Informationen zur deutschen Cloud:**

  https://www.microsoft.com/de-de/cloud/deutsche-cloud/

- **Informationen zu den Microsoft Azure Rechenzentren:**

  https://azure.microsoft.com/de-de/overview/datacenters/

Technische Sicherheitsvorkehrungen

SFTP, SQL, VPN, Dashboard, Passwörter & E-Mail Verifizierung

Secure FTP

Für jeglichen Datenverkehr stehen die höchstmöglichen Sicherheitsoptionen zur Verfügung. Für Kunden nutzen wir eine SFTP Verbindung und IP Schutz. Auf Wunsch können wir Ihnen Zertifikate hierzu vorweisen. Diese Ebene wird auch für Transfers zwischen Secure FTP und der SQL-Datenbank verwendet. Wir verwenden ein 15- oder 22-stelliges, zufällig generiertes Passwort mit einem zufälligen Passwortgenerator. Bei Bedarf können wir die öffentlichen Zugriffsschlüssel benutzen. Diese Verbindung wird nur von der IP-Adresse erlaubt, die vom Kunden bereitgestellt wird, zur Nutzung für den Austausch von Dateien.

Microsoft SQL Azure (RTM) - Firewall geschützt

Alle Datenbanken und Projekte unserer Kunden werden eigenständig gelagert und von denen anderer Kunden getrennt. Unsere Datenbank ist eine Azure-Datenbank, die hinter einer Azure Firewall positioniert ist. Azure erlaubt nur den Zugriff, wenn die IP-Adresse von der die Verbindung hergestellt wurde, enthalten ist. Darüber hinaus ist natürlich ein Benutzername und Passwort erforderlich.

Secure VPN

Die VPN-Verbindung ist eine Punkt-zu-Punkt Verbindung. die Verbindung ist verschlüsselt. Die VPN ist eine VPN-Verbindung in der Azure Umgebung zwischen den zwei Datenbanken.

Secure Dashboard

Das CFM-Dashboard läuf auf einem HTTPS-Server. Die Daten im Dashboard haben Standard-Sicherheit auf Login-Ebene mit einem Benutzernamen und einem (starken) Passwort. Wir verwenden speziell erzwungene starke Passwörter.

E-Mail Verifizierung

Eine periodische Erneuerung der Passwörter erfolgt innerhalb einer vorab definierten Anzahl von Tagen. Ein Konto arbeitet auf Basis eines einzigen Benutzer-Login. Ein starkes Passwort ist ein Passwort, das mindestens ein Zeichen enthält, das eine Zahl ist, ein Zeichen, das ein Großbuchstabe ist und ein Zeichen, das ein Symbol ist. Die Anzahl der Zeichen für Passwörter ist standardmäßig 8 (acht). Das Zurücksetzen eines Passworts ist möglich über die authentifizierte E-Mail-Adresse oder über die Management Funktion.

CYS Sicherheitspolitik

Interne Sicherheitsvorschriften zum Schutz der Kundendaten

- [x] CYS hat eine Partnerstrategie mit Local Heroes, die CFM-Kunden helfen, die Lösung zu implementieren, unter Berücksichtigung der lokalen Eigenheiten (inITova ist zertifizierter CYS-Partner für die DACH-Region)
- [x] CYS organisiert regelmäßige Sicherheits-Evaluierungen sowohl intern als auch mit Lieferanten
- [x] CYS hat eine aktive Strategie, um stets mit aktuellen Änderungen im Bereich Datenschutz konform zu bleiben
- [x] Mitarbeiter und Partner erhalten nur Zugang zu relevanten Systemen und erhalten nur für den Job relevante Benutzerrechte
- [x] Über alle Systeme hinweg arbeitet CYS nur mit persönlichen Konten und hält Log-Dateien an verschiedenen Orten
- [x] CYS hat eine aktive “Ausstiegsstrategie”, die die Schließung aller Konten und den Zugriff auf alle Datensysteme sicherstellt
- [x] Die Verschwiegenheit ist garantiert. Dies ist in allen Mitarbeiter-, Partner- und Lieferantenverträgen enthalten. Vertragsverletzung führt zu schweren Geldbußen
- [x] Updates auf CYS-eigenen Systemen und LIeferanten-Systemen werden aktiv protokolliert, um Fehlerkorrekturen und/oder Sicherheitsfragen zu vermeiden und/oder zu lösen

Weitere Informationen und rechtliche Aspekte

Eigentum, Verarbeitung, Löschung & Sicherung von Daten

Eigentum

inITova-Kunden bleiben immer Eigentümer aller Kundendaten. CYS und/oder Softwareanbieter bleiben Eigentümer der Software und der relevanten Quellcode(s)

Verarbeitung

Wir unterzeichnen mit Kunden eine Auftragsdatenverarbeitung (ADV), die den höchsten europäischen Sicherheitsstandards entspricht. Daneben hat CYS die erforderlichen Verfahren und Überwachungssysteme implementiert, um im Falle einer Bedrohung schnelle und adäquate Maßnahmen vornehmen zu können

Löschung & Sicherung

Auf Anfrage von Kunden wird inITova alle Kundenfeedback und/oder andere Forschungsdaten, die auf der Datenbank gesammelt wurden innerhalb einer angemessenen Frist von 5 (fünf) Werktagen entfernen. Im Falle einer Löschung wird eine Kopie der gesamten Datenbank dem Kunden auf einer gesicherten externen Festplatte übergeben

Bei Fragen kontaktieren Sie bitte:

Navid Tabrizi
n.tabrizi@initova.com
+49 221 29199 311

In Kooperation mit CYS BV Niederlande | *https://www.cys.group*